PATENT ABSTRACTS OF JAPAN

(11)Publication number : 10-247949
(43)Date of publication of application : 14.09.1998

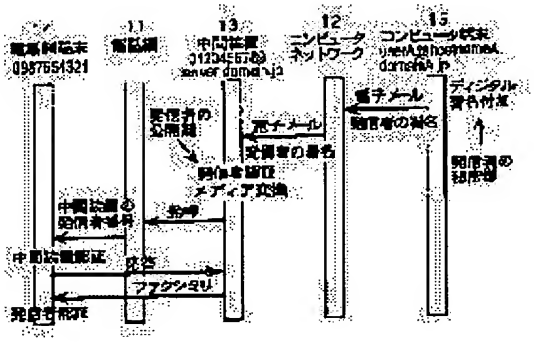
(51)Int.Cl. H04L 12/66
G09C 1/00
H04L 9/32
H04M 3/00
H04M 11/00
H04N 1/00
H04N 1/32
H04N 1/44

(21)Application number : 09-050137
(22)Date of filing : 05.03.1997

(71)Applicant : NIPPON TELEGR & TELEPH CORP <NTT>
(72)Inventor : YAMADA TOMOHIRO
TAKAHASHI ISAMU
SUZUKI AKIRA

(54) CALLER AUTHENTICATION METHOD

(57)Abstract:
PROBLEM TO BE SOLVED: To surely authenticate a caller in the case of communication between a telephone network terminal 14 and a computer terminal 15 via an intermediate device 13.
SOLUTION: A terminal 15 gives a digital signature to a message by using its private key and send the resulting message to an intermediate device 13, and the device 13 authenticates the signature by using a public key and when the signature passes the authentication, the device 13 converts the message into FAX image data and send the data to a terminal 14, the terminal 14 compares the caller number with a caller number of the device 13 stored in advance and receives the FAX data when they are coincident and the terminal 14 authenticates the caller of the terminal 15 from the reproduced image.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開平10－247949

(43)公開日　平成10年(1998)９月14日

(51)Int.Cl.[6]		識別記号	FI		
Ｈ０４Ｌ	12/66		Ｈ０４Ｌ	11/20	Ｂ
Ｇ０９Ｃ	1/00	６４０	Ｇ０９Ｃ	1/00	６４０Ｂ
Ｈ０４Ｌ	9/32		Ｈ０４Ｍ	3/00	Ｂ
Ｈ０４Ｍ	3/00			11/00	３０３
	11/00	３０３	Ｈ０４Ｎ	1/00	１０７Ａ

審査請求　未請求　請求項の数７　ＯＬ　（全 13 頁）　最終頁に続く

(21)出願番号　特願平9－50137

(22)出願日　平成９年(1997)３月５日

(71)出願人　000004226
日本電信電話株式会社
東京都新宿区西新宿三丁目19番２号

(72)発明者　山田　智広
東京都新宿区西新宿三丁目19番２号　日本電信電話株式会社内

(72)発明者　高橋　勇
東京都新宿区西新宿三丁目19番２号　日本電信電話株式会社内

(72)発明者　鈴木　晃
東京都新宿区西新宿三丁目19番２号　日本電信電話株式会社内

(74)代理人　弁理士　草野　卓

(54)【発明の名称】　発信者認証方法

(57)【要約】

【課題】　電話網端末１４とコンピュータ端末１５とが中間装置１３を介して通信する際に発信者認証を確実に行う。

【解決手段】　端末１５はメッセージにその秘密鍵によるディジタル署名を付けて中間装置１３へ送信し、装置１３は端末１５の公開鍵で署名を検証し合格すると、メッセージをＦＡＸ画像データに変換して端末１４へ送り、端末１４は発信者番号を予め記憶した装置１３の発信者番号と比較し、一致すればＦＡＸを受信し、その再生画像から端末１５の発信者認証を行う。

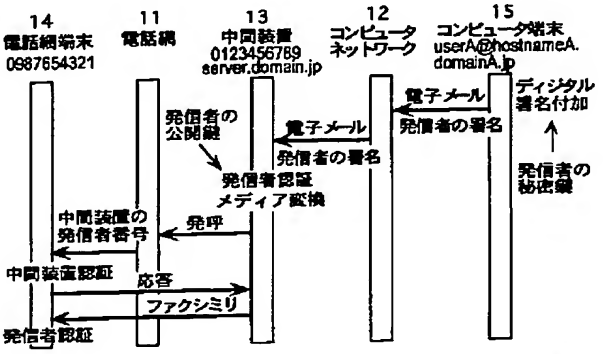


図６

1

【特許請求の範囲】

【請求項１】　電話網に収容された電話網端末と、コンピュータネットワークに収容されたコンピュータ端末とが、上記電話網と上記コンピュータネットワークのそれぞれとインタフェースをもつ中間装置（以下単に中間装置と記す）を介してメッセージを通信する際の発信者を認証する方法において、

上記コンピュータ端末からメッセージを発信する際に、そのメッセージにそのコンピュータ端末を使用する発信者のディジタル署名を付けて送信し、

上記中間装置で受信したメッセージの署名を認証することを特徴とする発信者認証方法。

【請求項２】　上記中間装置の発信者番号を上記電話網端末に記憶しておき、

上記電話網端末は上記中間装置から通信要求があると、その発信者番号を上記記憶した発信者番号とを照合して中間装置の認証を行うことを特徴とする請求項１記載の発信者認証方法。

【請求項３】　上記電話網端末は、上記発信者番号の照合が合格すると、上記中間装置からメッセージと共に通知された上記コンピュータ端末の発信者情報により発信者の認証を行うことを特徴とする請求項２記載の発信者認証方法。

【請求項４】　上記中間装置に受信したメッセージのメッセージＩＤを記憶し、

上記コンピュータ端末はその送信メッセージにメッセージＩＤを与え、このメッセージＩＤに対しても上記ディジタル署名を行い、

上記中間装置は上記コンピュータ端末からのメッセージ中のメッセージＩＤをそれ以前記憶した上記メッセージＩＤと比較し、一致すると、不正メッセージとして処理することを特徴とする請求項１乃至３の何れかに記載の発信者認証方法。

【請求項５】　電話網に収容された電話網端末と、コンピュータネットワークに収容されたコンピュータ端末とが、上記電話網と上記コンピュータネットワークのそれぞれとインタフェースをもつ中間装置（以下単に中間装置と記す）を介してメッセージを通信する際の発信者を認証する方法において、

上記中間装置は上記電話網端末より受信したメッセージを、これに対し中間装置のディジタル署名を付けて上記コンピュータ端末へ送信し、

上記コンピュータ端末は受信したメッセージの署名を認証することを特徴とする発信者認証方法。

【請求項６】　上記電話網端末の発信者番号を上記中間装置に記憶しておき、

上記中間装置は上記電話網端末からの通信要求があると、その発信者番号を上記記憶した発信者番号と照合して発信者の認証を行うことを特徴とする請求項５記載の発信者認証方法。

2

【請求項７】　上記メッセージの署名の認証に合格すると、上記中間装置からメッセージと共に通知された上記電話網端末の発信者情報により発信者の認証を行うことを特徴とする請求項５又は６記載の発信者認証方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】この発明は、コンピュータネットワークと電話網の端末間で相互にメッセージ通信を行う通信における発信者の認証方法に関するものである。

【０００２】

【従来の技術】図１２に示すように公衆電話網１１とコンピュータネットワーク１２とのそれぞれにインタフェースをもつ中間装置（以下単に中間装置と記す）１３が設けられ、電話網１１に収容された電話網端末１４とコンピュータネットワーク１２に収容されたコンピュータ端末１５とが中間装置１３を介してメッセージを通信する通信方法が知られている。

【０００３】従来、このようなコンピュータネットワーク１２と電話網１１の端末１５，１４間で相互にメッセージ通信を行うサービスでは、課金等のための発信者認証を行う方法として、目的に応じて主に次の２つの方法が取られている。第１の方法は、予め中間装置１３に電子メールアドレスを登録し、コンピュータネットワーク１２側からの電子メールを中間装置１３を経由して電話網端末としてのファクシミリ端末１４へ送信する場合は、図１に示すように、発信コンピュータ端末１５から中間装置１３に電子メールが送られて来ると、中間装置１３は電子メール内の発信端末１５のメールアドレスを予め登録した電子メールアドレスと照合することにより発信者認証を行い、その認証に合格すればコンピュータ端末１５より受信した電子メール内のテキスト（文字）や画像などのメッセージをファクシミリ信号に変換し、つまりメディア変換を行って着信側へ電話網のファクシミリ端末１４へ送信する。中間装置１３を介してファクシミリ端末１４に着信があると、ファクシミリ端末１４の受信者はファクシミリ端末１４の再生画像中のメッセージに添付されている前記電子メールアドレスにより発信者の確認を行う。

【０００４】また、電話網端末１４側からファクシミリをコンピュータ端末１５に送信する場合は図２に示すように中間装置１３においては、端末１４から受信したファクシミリに対しては特に発信者認証を行なわず、そのファクシミリ信号を電子メールの形式にメディア変換して着信側のコンピュータ端末１５へ送信する。この電子メールを受信したコンピュータ端末１５の受信者は端末１４の発信者が付加したカバーページにより発信者の確認を行う。

【０００５】第２の方法は、予め中間装置１３に発信者を認証するためのＩＤ（利用者識別情報）とパスワード

3

を登録し、コンピュータネットワーク１２側からの電子メールを中間装置１３を経由して電話網１１のファクシミリ端末１４に送信する場合は、図３に示すように、発信コンピュータ端末１５で発信者を認証するためのＩＤとパスワードを電子メールに添付して、中間装置１３に対して電子メールを送信し、中間装置１３は受信した電子メール内のＩＤとパスワードを予め登録したＩＤとパスワードと照合することにより発信者認証を行い、認証に合格すればその電子メールのメッセージをファクシミリ信号に変換して電話網のファクシミリ端末１４に送信する。ファクシミリ端末１４の受信者はファクシミリ端末１４の再生画像メッセージに付加されている発信者のＩＤにより発信者の確認を行う。

【０００６】また、電話網１１側からファクシミリをコンピュータ端末１５へ送信する場合は、図４に示すように、発信者がＰＢ音で発信者を認証するためのＩＤとパスワードをファクシミリ端末１４より入力し、中間装置１３はその入力されたＩＤとパスワードを予め登録したＩＤとパスワードと照合することにより発信者認証を行い、これに合格するとその後送られて来たファクシミリを電子メールに変換してコンピュータ端末１５へ送信する。コンピュータ端末１５の受信者は受信した電子メールのメッセージに付加されている発信者ＩＤにより発信者の確認を行う。

【０００７】

【発明が解決しようとする課題】従来の第１の方法では、発信者の電子メールアドレスが漏洩した場合、第３者が不正に発信者の電子メールアドレスを偽装してメッセージの送信を行うことが可能であり、発信者および受信者に不利益になる場合がある。また、発信者が送信したメッセージを第３者が不正に改ざんし、発信者および受信者に不利益になる場合があるという問題点があった。更に、電話網１１からファクシミリをコンピュータ端末へ送信する際には中間装置１３で認証を行わないため、第３者が不正にファクシミリを送信することにより、中間装置１３の管理者に不利益をもたらすおそれがあり、また、発信者が特定できないメッセージが受信者に送信されることにより、受信者の不利益になるおそれがあるという問題点があった。

【０００８】従来の第２の方法では、従来の第１の方法と同様に、第３者が不正に発信者のＩＤとパスワードを偽装しメッセージの送信を行うことが可能であり、発信者および受信者に不利益になる場合がある。また、発信者が送信したメッセージを第３者が不正に改ざんし、発信者および受信者に不利益になる場合があるという問題点があった。更に、電話網１１からファクシミリをコンピュータ端末１５へ追信する際にも、第３者が不正に発信者のＩＤとパスワードを偽装使用してメッセージの送信を行うことが可能であり、発信者および受信者に不利益になる場合があるという問題点があった。

4

【０００９】この発明は、第３者が発信者になりすます、あるいは第３者がメッセージを改ざんすることにより発信者および受信者の不利益になるという問題点および第３者が不正にファクシミリを送信することにより中間装置の管理者の不利益になるという問題点を解決した、発信者認証方法を提案することを目的とする。

【００１０】

【課題を解決するための手段】この発明は、コンピュータ端末より発信する場合はディジタル署名を行い、中間装置でメッセージに付加されたディジタル署名を使用して発信者認証を行うことで、第３者によるなりすましの防止およびメッセージに対する改ざんの検出を可能とし、電話網端末よりの発信に対しては電話網より通知される発信者番号を使用して発信者認証を行うことで、第３者によるなりすましの防止を可能とし、電話網端末に着信があると、その受信者は中間装置１３より通知される中間装置の発信者番号および受信メッセージ中の発信者情報を使用して発信者認証を行うことにより発信者の確認を可能とし、コンピュータ端末に着信があるとその受信者は受信メッセージに付加された中間装置のディジタル署名を使用して中間装置の認証を行い、メッセージ内の発信者情報を取り出すことで、発信者の確認を可能とする。

【００１１】

【作用】中間装置での認証において、コンピュータネットワークに接続されている発信者に対しては、メッセージに付加されたディジタル署名を使用して発信者認証を行うことで、第３者が発信者の電子メールアドレスを偽ったとしても、ディジタル署名が異なれば、不正なメッセージとして破棄することができる。また、ディジタル署名は発信者のみが作成できかつメッセージ毎に異なる為、第３者が不正にディジタル署名を複製した場合およびメッセージの一部が改ざんされた場合であっても検出することが可能になる。また、電子メール装置により一意に付与されるメッセージＩＤに対してもディジタル署名を施すことにより、同一のメッセージＩＤを持つメッセージを破棄することで、メッセージ全体を不正に複製した場合であっても検出が可能となる。電話網に接続されている発信者に対しては、発信者からではなく、電話網より通知される発信者番号を使用して発信者認証を行うことで、第３者が不正に成りすますことを防ぐことが可能になる。受信者での認証においても、電話網に接続されている受信者は、予め中間装置の発信者番号のみを取得しておくことで、電話網より通知される中間装置の発信者番号およびメッセージ中の発信者情報を使用して発信者認証を行うことにより発信者の確認が可能となり、コンピュータネットワークに接続されている受信者は、予め中間装置の公開鍵のみを取得しておくことで、中間装置のディジタル署名を使用して中間装置の認証を行い、メッセージ内の発信者情報を取り出すことで、発

5

信者の確認が可能となる。

【００１２】

【発明の実施の形態】

実施例１

図１Ａにこの発明が適用される通信システムの一例を示し、図１２と対応する部分に同一符号を付けてある。電話網１１は発信者番号通知手段２１を備えているものである。電話網端末１４は電話網１１との信号の送受を行う通信制御手段２２を備え、またこの例ではファクシミリ端末の場合であり、画像入出力手段２３を備え、この発明では更に、受信メッセージから発信者番号抽出手段２４、更に中間装置１３の発信者番号を記憶する蓄積手段２５を備えている。

【００１３】中間装置１３は電話網１１、コンピュータネットワーク１２とそれぞれ通信の送受を行う通信制御手段（インタフェース）２６，２７を備えている他に、この発明では、発信者番号抽出手段２８、送信メッセージにディジタル署名を付加する手段２９、メディア変換手段３０、受信ディジタル署名を照合（検証）する手段３１、更に、ディジタル署名、とその検証に必要な公開鍵、秘密鍵を記憶する蓄積手段３２を備えている。

【００１４】コンピュータ端末１５はコンピュータネットワーク１２との通信の送受を行う通信制御手段３３、電子メールの入出力手段３４を備えている他に、この発明では送信メッセージにディジタル署名を付加する手段３５、受信ディジタル署名を照合（検証）する手段３６、ディジタル署名、その検証に必要な公開鍵、秘密鍵を記憶する蓄積手段３７を備えている。

【００１５】この発明ではディジタル署名を利用するが、これに必要とする鍵の取得について、図２を参照して説明する。中間装置１３は公開鍵と秘密鍵の対を生成して、公開鍵を、認証局３９に登録すると共に秘密鍵を蓄積手段３２に記憶する。コンピュータ端末１５は認証局３９から中間装置１３の公開鍵を取得し、また公開鍵と秘密鍵の対を生成し、その公開鍵を認証局３９に登録すると共に秘密鍵を蓄積手段３７に記憶し、更に自己の名前などの利用者情報（ＩＤ）に対し、コンピュータ端末１５の秘密鍵でディジタル署名を添付して、これを中間装置１３の公開鍵で暗号化して中間装置１３へ送信する。中間装置１３はその受信データを中間装置１３の秘密鍵で復号化し、また、認証局３９からコンピュータ端末１５の公開鍵を取得し、この公開鍵で前記復号化ディジタル署名を検証し、合格すれば、その受信した復号化したコンピュータ端末１５の利用者情報を蓄積手段３２に蓄積登録し、その登録結果を示すメッセージを作成して、これに対し中間装置１３の秘密鍵で署名し、その署名付登録結果メッセージをコンピュータ端末１５の公開鍵で暗号化してコンピュータ端末１５へ送信する。コンピュータ端末１５は受信した暗号化データを秘密鍵で復号化し、その復号化された署名を中間装置１３の公開鍵

6

で検証し、その登録内容を確認する。

【００１６】この実施例１はコンピュータ端末１５から、中間装置１３を経由して、電話網端末１４に対してメッセージを送信する場合である。この場合電子メール装置（コンピュータ端末）１５を使用する発信者は予め、例えば図２で説明した方法により、認証に必要な情報である発信者（コンピュータ端末１５）の加入者情報を中間装置１３内の加入者情報蓄積手段３２に登録しておき、中間装置１３は発信者の認証に必要なコンピュータ端末１５の公開鍵を取得し、加入者情報蓄積手段３２に記憶しておく、また、電話網端末１４、この実施例ではファクシミリ端末を使用する受信者は予め、中間装置１３の認証に必要な中間装置１３の発信者番号を情報蓄積手段２２に蓄積しておく。

【００１７】コンピュータ端末１５からメッセージを送信する際に、メール入出力手段３４によりメッセージを作成し、ディジタル署名付加手段３５により、前記作成したメッセージに対して、コンピュータ端末１５の秘密鍵を使用し、発信者のディジタル署名を付加する。このディジタル署名を付加したメッセージは、通信制御手段３３により、中間装置１３に対して送信される。

【００１８】中間装置１３はこのメッセージを通信制御手段２７より受信し、ディジタル署名照合手段３１により、予め蓄積手段３２に蓄積されたコンピュータ端末１５の公開鍵を使用して、メッセージに付加されたディジタル署名の照合を行う。照合を行った結果、ディジタル署名が確かに発信者のものであり且つ、改ざんされていない場合は、正しいメッセージであると解釈し、メディア変換手段３０により、電子メールの内容をファクシミリ画像に変換する。ディジタル署名が不正であった場合はメッセージを破棄する。メディア変換を行ったメッセージは、通信制御手段２６により、電話網端末１４に対して送信される。中間装置１３から電話網端末１４に対する発呼があると、電話網１１は発信者情報通知手段２１により、中間装置１３の発信者番号を受信端末１４に通知する。受信端末１４は発信者番号抽出手段２４により発信者番号を抽出し、情報蓄積手段２５に蓄積されている中間装置１３の発信者番号により、中間装置１３からの着呼であることを確認したのち、通信制御手段２２によりファクシミリの受信を行う。受信したファクシミリの再生画像は発信者の情報が付加されている為、発信者が中間装置１３に登録されている発信者であることが確認できる。

【００１９】なお、コンピュータ端末１５で作成する電子メールは例えば図３に示すようなものである。即ち、まず発信者アドレス６１が記述され、次に以下の記述のフォーマット６２（この例ではＭＩＭＥバージョン１．０）が示され、これに相手先（受信者）アドレス６３が続き、更に主題６４がこの例では日本語ＪＩＳコードでテストであることが記述され、次に内容形式６５がこの

例ではマルチパート／混合で境界を“・・・７４２９５９Ｆ６２１８Ｅ”で示し、この境界６６を付けて、内容形式６７がこの例ではテキスト／通常、文字はＪＩＳ規格コードであることが示され、更に内容変換符号化６８がこの例では７ビット符号であることが示された後にメッセージ内容であるテキスト６９が記述される。次の境界７０の後に内容形式７１がこの例では画像であり、そのフォーマットがｇｉｆであることが示され、その内容変換符号化７２がこの例ではｂａｓｅ６４によることが示され、次にその符号化された画像データ７３が記述され、その終りに境界７４が付けられる。

【００２０】このメッセージに対し署名した電子メールは例えば図４に示すようになる。つまり発信アドレス６１、記述フォーマット６２、着信アドレス６３、主題６４は図３と同一であり、次の内容形式６５で、マルチパート、署名付きとなり、かつ境界が“Ｎｅｘｔ　Ｐａｒｔ　Ｌｅｖｅｌ－１－１５２６３３”となり、署名アルゴリズムがｐｇｐ－ｍｄ５であることが記述され、境界６６の次の内容形式６７でメッセージであることとそのフォーマットｒｆｃ８２２が記述された後に、図３中の全メッセージの記述７５がなされ、その終りの境界７６に続く内容形式７７にｐｇｐ法による署名であり、その署名データ７８が続き、最後に境界７９が付けられている。

【００２１】中間装置１３内のメディア変換手段３０では、この例では受信メッセージ中のテキスト（文字）６９が例えば図５に示すようにファクシミリ画像のデータに変換され、また画像メッセージ７３も図５に示すようにファクシミリ画像のデータに変換される。この場合、両画面の左上端部に発信者アドレスと主題とが画像データとして付け加えられる。

【００２２】上述した実施例の処理の流れを図６に示す。コンピュータ端末１５では作成したメッセージに対し、端末１５の秘密鍵で署名し、この署名付きメッセージを電子メールとして中間装置１３へ送る。中間装置１３は端末１５の公開鍵で署名を検証し、合格すれば、そのメッセージをメディア変換して電話網端末（ファクシミリ端末）１４を呼出し、端末１４は中間装置１３の発信者番号を確認し、正しければ、中間装置１３に応答し、ファクシミリを受信する。そのファクシミリの再生画像中の発信アドレスから、その発信者、つまりコンピュータ端末１５から発信されたものであることを確認する。

実施例２

図７にこの発明の実施例を示す。これは電話網端末１４から中間装置１３を経由して、コンピュータ端末１５にメッセージを送信する場合である。

【００２３】電話網端末としてのファクシミリ端末１４を使用する発信者は予め、認証に必要な自分の発信者番号を中間装置１３内の加入者情報蓄積手段３２に登録を

行う。また、コンピュータ端末の電子メール装置１５を使用する受信者は、中間装置１３の認証に必要な中間装置の公開鍵を認証局から取得し、情報蓄積手段３７に蓄積しておく。ファクシミリ端末１４からコンピュータ端末１５へメッセージを送信する際に、ファクシミリ入出力手段２３により例えば図８に示すようなファクシミリ画像を入力する。入力されたファクシミリ画像は、通信制御手段２２により、中間装置１３に対して送信される。その際に端末１４から中間装置１３に対して発呼があると、電話網１１は発信者情報通知手段２１により、発信端末１４の発信者番号を中間装置１３に通知する。中間装置１３は、発信者番号抽出手段２８により、発信端末の発信者番号を抽出した後、加入者情報蓄積手段３２に蓄積されている端末１４の発信者番号と照合する。照合した結果が正しい場合は通信制御手段２６により、ファクシミリの受信を行う。発信者番号が一致しない場合は不正な着呼と判断し、受信を行わない。受信したファクシミリ画像は、メディア変換手段３０により例えば図９に示すような電子メールのフォーマットに変換する。この電子メールは図３の場合と同様に、発信アドレス６１、記述フォーマット６２、受信アドレス６３、主題６４（この例ではＦＡＸ）であり、内容形式６５が記述された後の境界６６の次は図３中の画像メッセージ部分と対応したものが続く。

【００２４】この電子メールフォーマットに変換されたメッセージは、ディジタル署名付加手段２９により、図４に示した場合と同様に中間装置１３のディジタル署名を付加する。ディジタル署名を付加したメッセージは、通信制御手段２７によりコンピュータ端末（電子メール装置）１５に送信される。コンピュータ端末１５は通信制御手段３３により、メッセージを受信した後、ディジタル署名照合手段３６により、情報蓄積手段３７に予め取得した中間装置１３の公開鍵を使用して、メッセージに付加されたディジタル署名の照合を行う。照合した結果が正しければ、その電子メール中のＦｒｏｍ行に記載されている発信者情報（アドレス）により、発信者が中間装置１３に登録されている発信者であることが確認できる。

実施例３

この実施例は、コンピュータ端末１５から中間装置１３を経由して、電話網端末１４に対してメッセージを送信する場合で、実施例１との違いは、発信者が作成したメッセージにのみディジタル署名を施すのではなく、コンピュータ端末１５内の通信制御手段３３により付加されるメッセージＩＤに対してもディジタル署名を施し、これにより、メッセージＩＤが改ざんされることがなくなり、メッセージＩＤにより、一意にメッセージの識別を行うことを可能とする。これを実現するため、中間装置１３内に受信したメッセージＩＤを記憶するＩＤ蓄積手段４１が図１に実線で示すように設ける。

【００２５】この処理手順を図１０に示す。実施例と同様にコンピュータ端末１５の公開鍵を中間装置１３に登録し、また中間装置１３の発信者番号を電話網端末１４の情報蓄積手段２５に蓄積しておく。コンピュータ端末１５からメッセージを送信する際に、入出力手段３４によりメッセージを作成し、このメッセージに対して通信制御手段３３により、メッセージＩＤを付加する。ディジタル署名付加手段３５により、前記メッセージに対して、自分のディジタル署名を付加して通信制御手段３３により、中間装置１３に対して送信する。

【００２６】メッセージを受信した中間装置１３は、ディジタル署名照合手段３１により、予め蓄積手段３２に蓄積された利用者情報を使用して、メッセージに付加されたディジタル署名の照合を行う。ディジタル署名が不正であった場合はメッセージを破棄する。照合を行った結果、ディジタル署名が確かに発信者のものであり且つ、改ざんされていない場合は、正しいメッセージであると解釈し、次にＩＤ蓄積手段４１に蓄積されている全てのメッセージＩＤと受信メッセージ中のメッセージＩＤとの比較を行う。メッセージＩＤが異なる場合は、メッセージ中のメッセージＩＤをＩＤ蓄積手段４１に蓄積し、メディア変換手段３０により、電子メールの内容を図５に示したようなファクシミリ画像のデータに変換する。前記メッセージＩＤの比較の結果、そのメッセージＩＤがすでに、メッセージＩＤ蓄積手段４１に存在する場合は、この受信メッセージは不正に複製されたものと判断し、そのメッセージを破棄する。メディア変換を行ったメッセージは、通信制御手段２６により、電話網端末１４とのファクシミリ端末へ送信する。この後の処理は実施例１と同様である。

【００２７】公開鍵の取得方法としては例えば図１１に示すように行ってもよい。図２の場合と同様に中間装置１３、コンピュータ端末１５はそれぞれ公開鍵と秘密鍵の対を生成し、公開鍵と自分の情報とをそれぞれ認証局３９に登録を行う。その際に登録内の確認証明書を認証局３９から発行してもらい、その証明書を蓄積手段３２，３７にそれぞれ蓄積しておく。コンピュータ端末１５はその利用者情報を中間装置１３に登録するために、まず中間装置１３から中間装置の証明書を取得し、また認証局３９から認証局３９の公開鍵を取得し、この公開鍵を用いて、取得した中間装置の証明書の認証を行い、その認証に合格すれば、その証明書から、中間装置１３の公開鍵を取出し、その公開鍵でコンピュータ端末１５の利用者情報を暗号化し、これに対するコンピュータ端末１５の秘密情報で署名を行い、その署名付き暗号化利用者情報と、コンピュータ端末の証明書を中間装置１３へ送信する。

【００２８】中間装置１３では、認証局３９から認証局の公開鍵を受取り、この公開鍵で受信したコンピュータ端末の証明書を認証し、これに合格すれば、その証明書

からコンピュータ端末１５の公開鍵を取出し、その公開鍵を蓄積手段３２に蓄積すると共にその公開鍵で受信した暗号化利用者情報の署名を検証し、これに合格すれば、その暗号化利用者情報を中間装置１３の秘密鍵で復号化し、その利用者情報の内容に間違いがないかを確認した後、利用者情報を蓄積手段３２に記憶する。その登録結果メッセージをコンピュータ端末１５の公開鍵で暗号化し、その暗号化登録結果を、これに対し中間装置１３の署名を付け、更に中間装置の証明書も付けてコンピュータ端末１５へ送る。

【００２９】コンピュータ端末１５は同様にして、受信登録結果の署名を中間装置の公開鍵で検証し、更に、コンピュータ端末１５の秘密鍵で復号化して登録内容を確認する。このように証明書を発行してもらい、コンピュータ端末１５（あるいは中間装置１３）から送信するメッセージにそのコンピュータ端末１５（中間装置１３）の証明書を付けて送信すれば、受信した中間装置１３（コンピュータ端末１５）は受信した証明書からコンピュータ端末１５（中間装置１３）の公開鍵を得ることができる。従って中間装置１３は認証局３９からコンピュータ端末１５の公開鍵を取得する必要はない。

【００３０】

【発明の効果】以上説明したように、請求項１乃至４の発明によれば、コンピュータ端末１５からのメッセージの受け付けにおいて、中間装置１３で第３者によるなりすましの防止およびメッセージに対する改ざんの検出が可能となり、また、第３者によるメッセージの複製を検出することが可能となり、発信者への課金が正しく行われるという経済的効果がある。

【００３１】また、請求項５乃至７の発明によれば、電話網端末１４からのメッセージの受け付けにおいて、中間装置１３で第３者によるなりすましの防止が可能となり、発信者への課金が正しく行われるという経済的効果がある。また、請求項２の発明によれば、受信端末における発信者認証において、予め中間装置の情報を取得しておくだけで、発信者が正しいかいなかの確認が可能になるというサービス性を向上させる効果がある。

【図面の簡単な説明】

【図１】この発明方法が適用される通信システムの例を示すブロック図。

【図２】この発明に用いられる公開鍵取得方法の手順を示す図。

【図３】コンピュータ端末１５で作られたメッセージの例を示す図。

【図４】コンピュータ端末１５で図３のメッセージをディジタル署名した電子メールの例を示す図。

【図５】図３のメッセージをファクシミリ画像に変換した例を示す図。

【図６】請求項２の発明の実施例のシーケンスを示す図。

11

【図７】請求項５の発明の実施例のシーケンスを示す図。

【図８】送信ファクシミリ画像の例を示す図。

【図９】図８のファクシミリ画像を電子メッセージに変換した例を示す図。

【図１０】請求項４の発明の実施例のシーケンスを示す図。

【図１１】公開鍵取得の他の方法のシーケンスを示す図。

【図１２】この発明方法が適用される通信システムの例

12

を示す図。

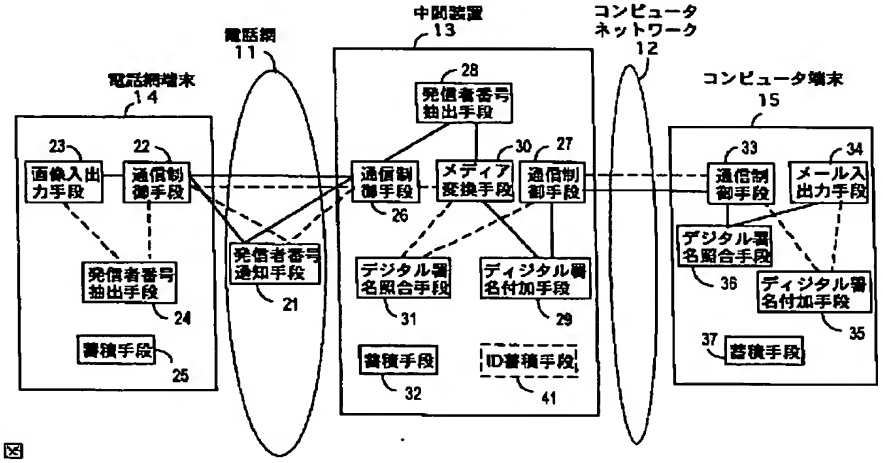
【図１３】従来の電話網端末からの発信した場合のシーケンスを示す図。

【図１４】従来のコンピュータ端末から発信した場合のシーケンスを示す図。

【図１５】従来の電話網端末からの発信した場合のシーケンスを示す図。

【図１６】従来のコンピュータ端末から発信した場合のシーケンスを示す図。

【図１】



図一

【図６】

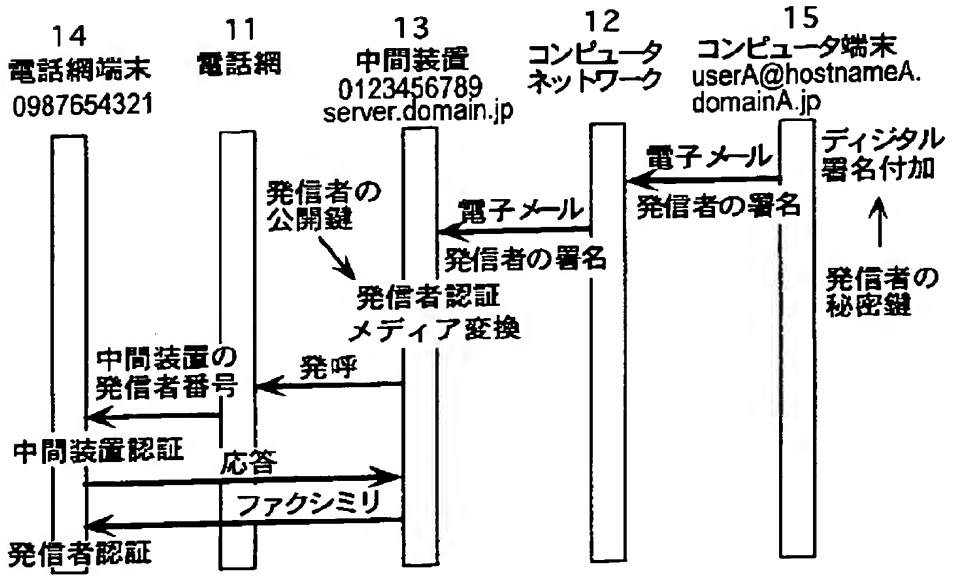


図６

【図２】

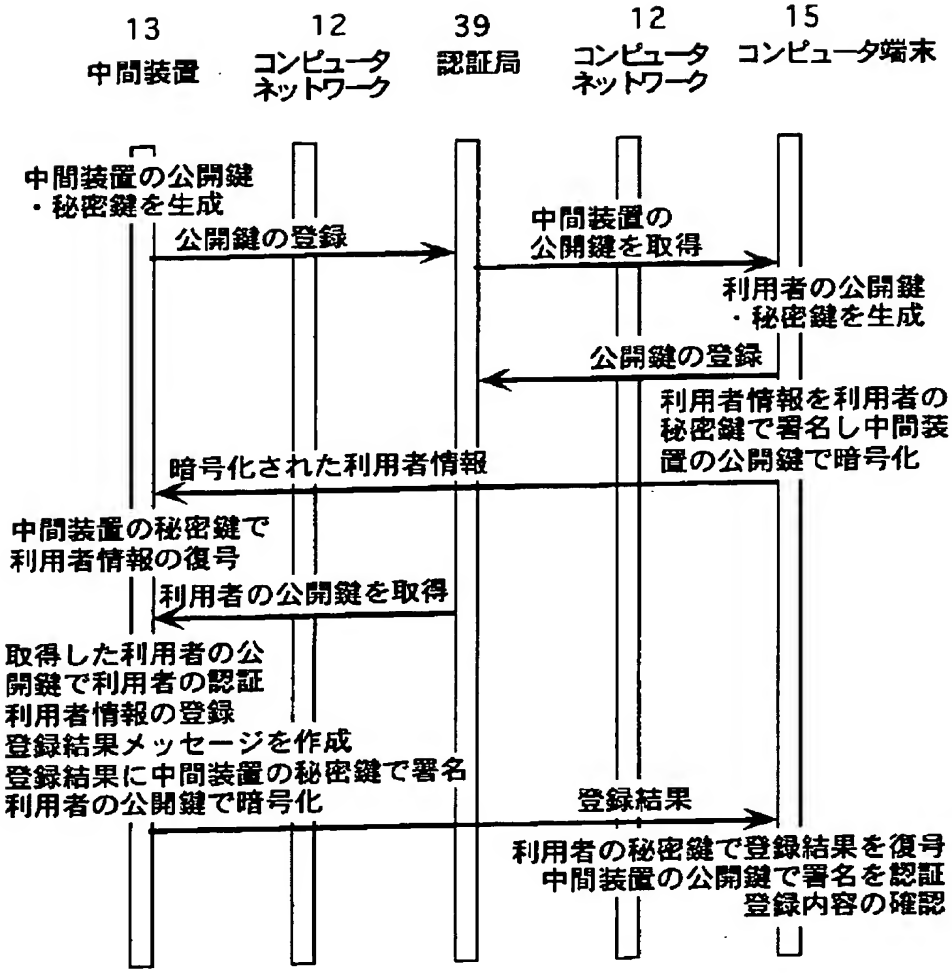

13
中間装置
12
コンピュータネットワーク
39
認証局
12
コンピュータネットワーク
15
コンピュータ端末
中間装置の公開鍵・秘密鍵を生成
公開鍵の登録
中間装置の公開鍵を取得
利用者の公開鍵・秘密鍵を生成
公開鍵の登録
利用者情報を利用者の秘密鍵で署名し中間装置の公開鍵で暗号化
暗号化された利用者情報
中間装置の秘密鍵で利用者情報の復号
利用者の公開鍵を取得
取得した利用者の公開鍵で利用者の認証
利用者情報の登録
登録結果メッセージを作成
登録結果に中間装置の秘密鍵で署名
利用者の公開鍵で暗号化
登録結果
利用者の秘密鍵で登録結果を復号
中間装置の公開鍵で署名を認証
登録内容の確認

図２

【図１２】

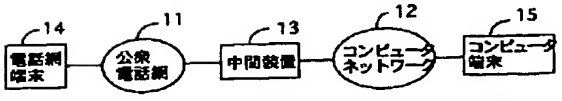

14
電話網端末
11
公衆電話網
13
中間装置
12
コンピュータネットワーク
15
コンピュータ端末

図12

【図３】

```
61 From: userA@hostnameA.domainA.jp
62 MIME-Version: 1.0
63 To: 0987654321@server.domain.jp
64 Subject: =?iso-2022-jp?B?GyRCJUYlOSVlGyhK?=
65 Content-Type: multipart/mixed; boundary="·····742959F6218E"

   This is a multi-part message in MIME format.

66 ·····742959F6218E
67 Content-Type: text/plain; charset=iso-2022-jp
68 Content-Transfer-Encoding: 7bit

69 こんにちは。
   これはテストです。

70 ·····742959F6218E
71 Content-Type: image/gif; name="sample.gif"
72 Content-Transfer-Encoding: base64

   R0lGODlhewBaAPcAAP////Hu7Ofb0vfPqsDAwMXFxeG0k8uli
   KWlpYWFhXJpZFpaWkA/PjAwMBYVFQAAAAAAAAAAAAAAA
   AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
   <中略>
73 mDXSW8oSTgCv5yOtPMZVzKtd9AJFFgWaBTLXa5/7EPiWpURv
   R2PhV2dCtDzlZHB7PeFg78CiFg3mxUfEs4vPcnIZxFjQdr+hy7
   byAkHXoUhdFKTKDD33JerRZUf9epfnWdykJ4Lhryf8U56viFg/
   kMVPPFczHMSaCDKC+MIRBYgbgjRUGQX4D2QbCs92sBSzbpVm
   Mi07230gs8lqloQ+ajzJgkBEx+0ABjLJkYwb98jHPvrxj4C8TUA
   AADs=

74 ·····742959F6218E····
```

図３

【図４】

```
61 From: userA@hostnameA.domainA.jp
62 MIME-Version: 1.0
63 To: 0987654321@server.domain.jp
64 Subject: =?iso-2022-jp?B?GyRCJUYlosvlGyhK?=
65 Content-Type: multipart/signed; boundary="Next_Part_Levl_1_152633";
   micalg=pgp-md5;
        protocol="application/pgp-signature"

66 ····Next_Part_Level_1_152633
67 Content-Type: message/rfc822

   From: userA@hostnameA.domainA.jp
   MIME-Version: 1.0
   To: 0987654321@server.domaine.jp
   Subject: =?iso-2022-jp?B?GyRCJUYlosvlGyhK?=
   Content-Type: multipart/mixed; boundary="·····742959F8218E"

   This is a multi-part meesage in MIME format.

   ·····742959F6218E
   Content-Type: text/plain; charset=iso-2022-jp
   Content-Transfer-Encoding: 7bit

   こんにちは。
75 これはテストです。

   ·····742959F6218E
   Content-Type: image/gif; name="faximage1.gif"
   Content-Transfer-Encoding: base64
   Content-Disposition: inline; filename="faximage1.gif"

   R0lGODlhawBaAPcAAP///Hu7Ofb0vfpqsDAwMXFxeG0k8uiiKWlpYWFhXJpZ
   FpaWkA/PjAwMBYVFQAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
   <中略>
   IFg/kMVPPFczHMSaCDKC+MIRBYgbgjRUGQX4D2QbCs92sBSzbpVmMI072
   30gs8lqloQ+ajzJgkBEx+0ABjLJkywb98jHPvrxj4C8TUAAADs=
   ·····742959F6218E····
76 ····Next_Part_Level_1_1512633
77 Content-Type: application/pgp-signature

   ·····BEGIN PGP SIGNATURE·····
   Version: 2.6.2i
78 IQBVAwUBMvWLWu8FlMT+s8kpAQFMCAH/dOXF1AkhNPzsyfffhDGicowz59z
   n6KmC2+MvJthCZlnuZYxEEY4emq8igDc9jiwemXnFQZ3TEYfGNUHYRTZbg==
   =g0b6
   ·····END PGP SIGNATURE·····
79 ····Next_Part_Level_1_152633-
```

図４

【図５】

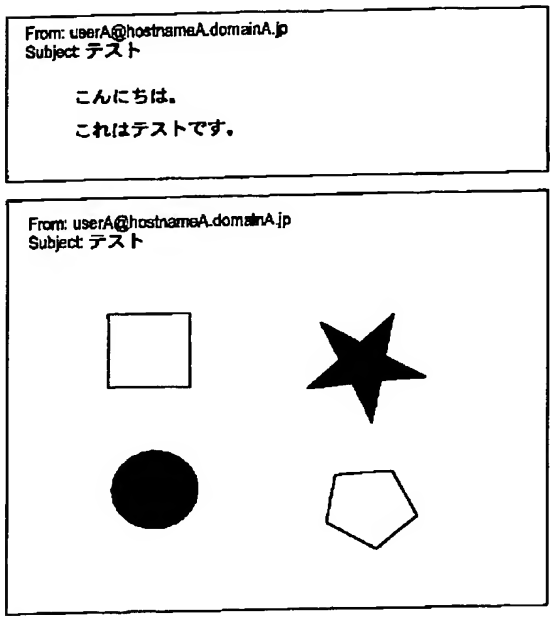


図５

【図８】

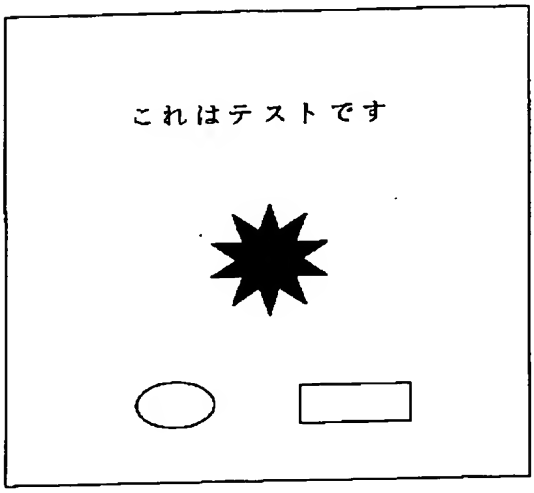


図８

【図７】

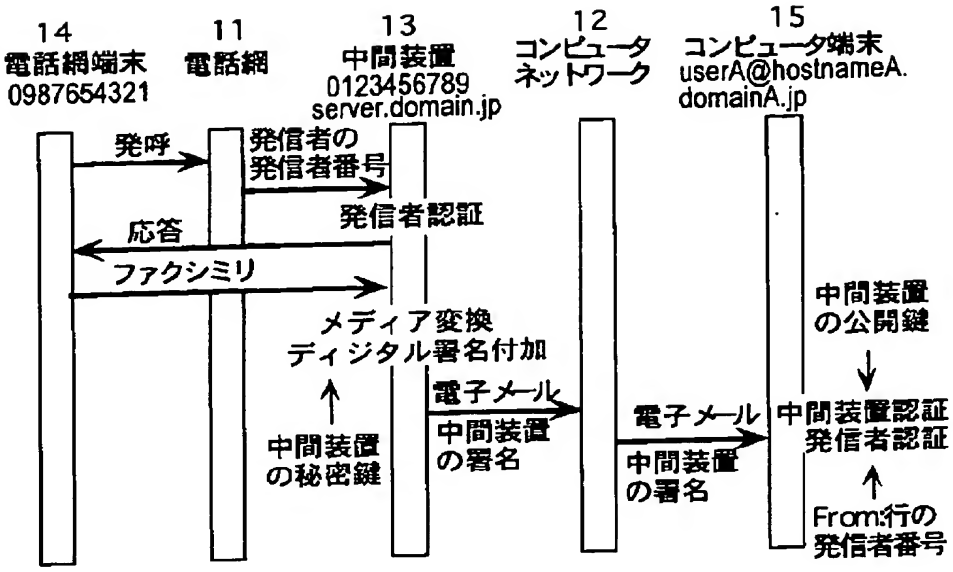


図7

【図９】

```
61 ─From: 0987654321@server.domainA.jp
62 ─MIME-Version: 1.0
63 ─To: userA@hostnameA.domain.jp
64 ─Subject: FAX
65 ─Content-Type: multipart/mixed; boundary="·····742959F6218E"

66 ─·····742959F6218E
71 ─Content-Type: image/gif; name="sample.gif"
72 ─Content-Transfer-Encoding: base64

73 ┌ R01GODdhwAagCIAAAP///wAAACwAAAAAwAagCAAC/4SPqcvtD6
   │ OctNqLs968+w+G4kiW5omm6sq27gvH8kzX9o3n+s73/g8MCofEovG
   │ ITCqXzKbzCY1SAqEZVYrNardcF/ULk7FkuuD7ACnw2iF+b2s82JOf
   │ lgv3f3fPw9DpEXVZen8fYmh5ih2KHX9wqZKSnFyAAldxZRlW15Seh
   │ o6OkW
   │ <中略>
   │ 9mRRNmXnfYoiVGVd9mVhVffjNWZptmZt9mZxNmd1dmd5bmd99
   │ meBNqRohXZoibZojfZokTZp1XZpmbZpnfZpoTZqpXZqqbZqrfZqs
   │ TZrtXZrubZrvfZrwTZsxXZsybZszfZs0TZt1XZt2bZt3fZt4TZu5XZu6b
   │ Zu7fZu8TZv9XZv+bZvfZvATdwBXdwCbdwDfdwETdxFXdxGbdxEf
   │ dxITdyJXdyKbdyLfdyMTdzNXdzObdzPfdzQTd0RXd0Sbd0Tfd0UTd
   └ 1VXdlg6AAAAA7

74 ─·····742959F6218E····
```

図９

【図１３】

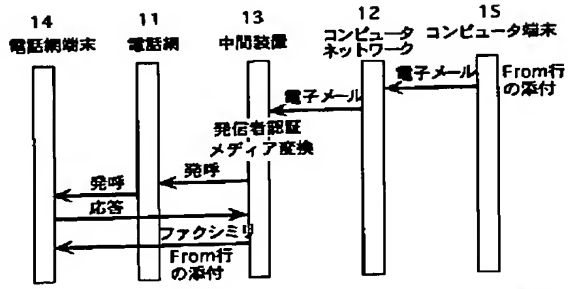


図13

【図１４】

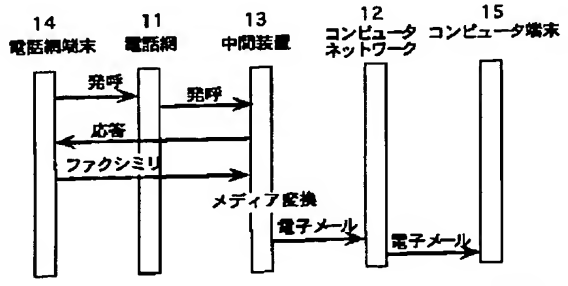


図14

【図１０】

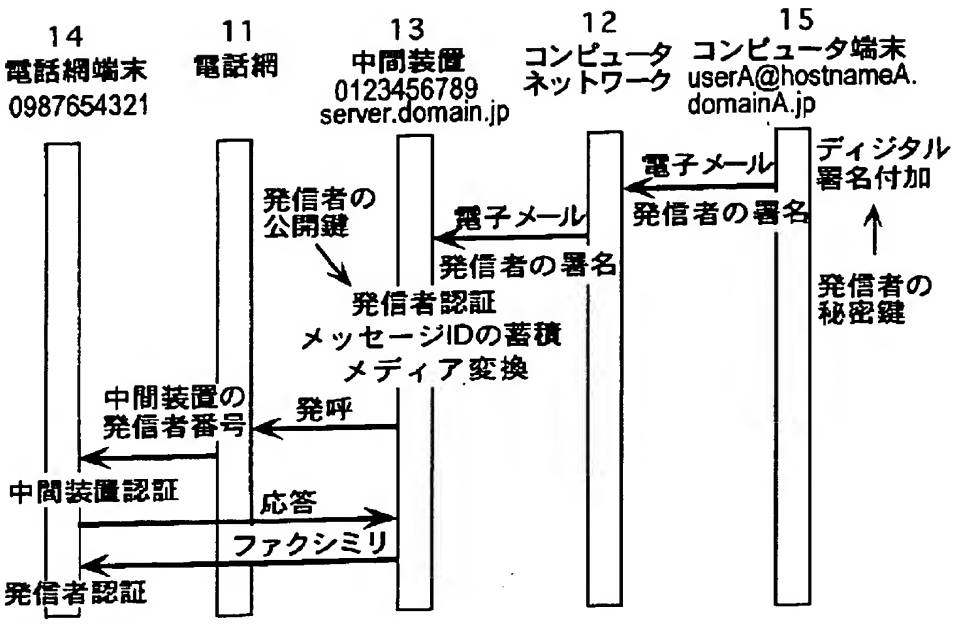


図１０

【図１５】

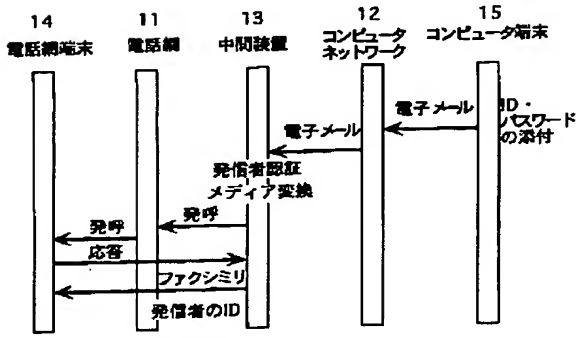


図15

【図１６】

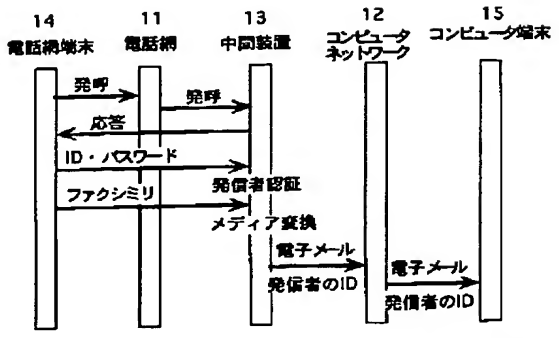


図16

【図１１】

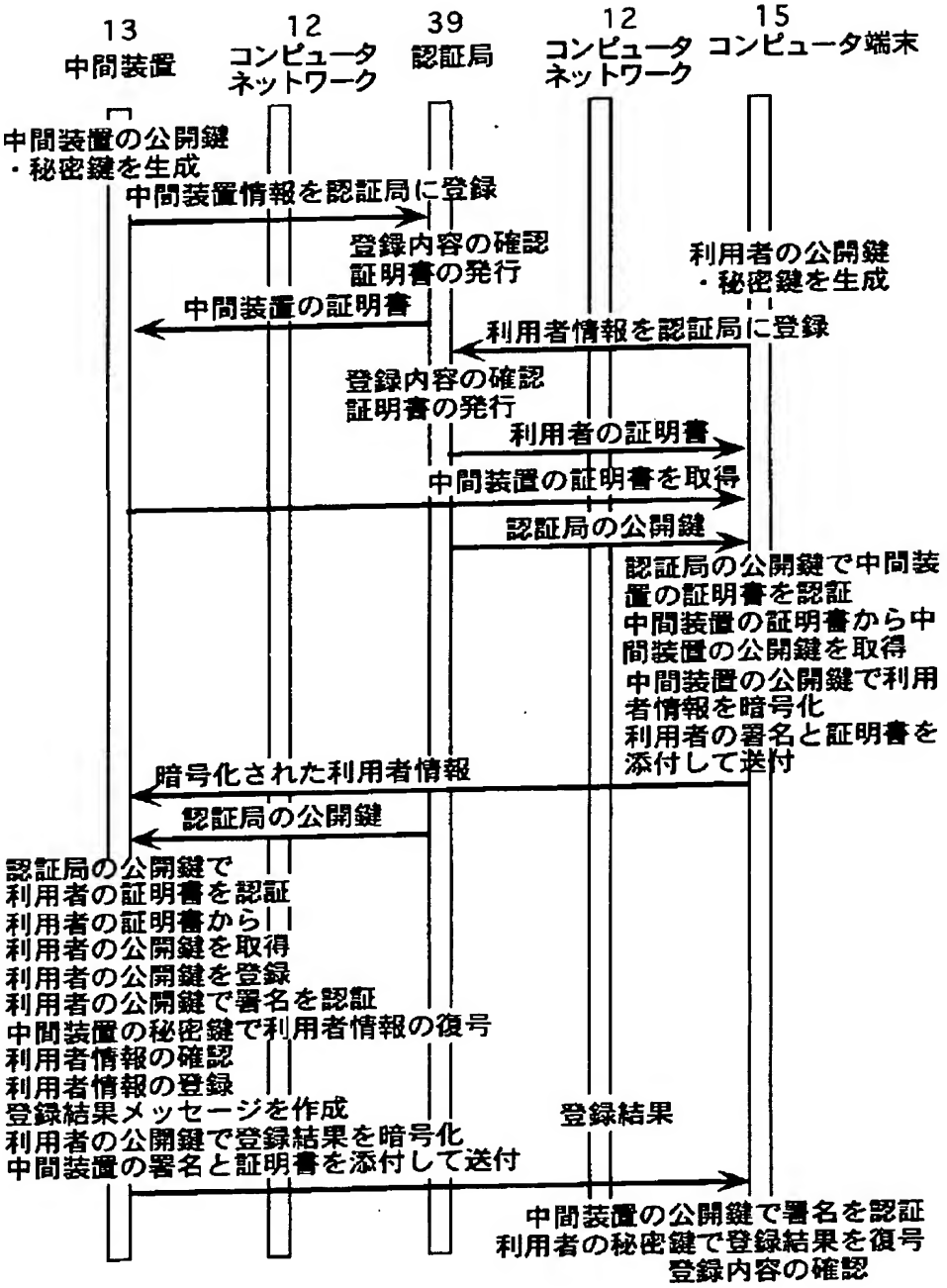

13
中間装置
12
コンピュータネットワーク
39
認証局
12
コンピュータネットワーク
15
コンピュータ端末
中間装置の公開鍵・秘密鍵を生成
中間装置情報を認証局に登録
登録内容の確認
証明書の発行
利用者の公開鍵・秘密鍵を生成
中間装置の証明書
利用者情報を認証局に登録
登録内容の確認
証明書の発行
利用者の証明書
中間装置の証明書を取得
認証局の公開鍵
認証局の公開鍵で中間装置の証明書を認証
中間装置の証明書から中間装置の公開鍵を取得
中間装置の公開鍵で利用者情報を暗号化
利用者の署名と証明書を添付して送付
暗号化された利用者情報
認証局の公開鍵
認証局の公開鍵で
利用者の証明書を認証
利用者の証明書から
利用者の公開鍵を取得
利用者の公開鍵を登録
利用者の公開鍵で署名を認証
中間装置の秘密鍵で利用者情報の復号
利用者情報の確認
利用者情報の登録
登録結果メッセージを作成
利用者の公開鍵で登録結果を暗号化
中間装置の署名と証明書を添付して送付
登録結果
中間装置の公開鍵で署名を認証
利用者の秘密鍵で登録結果を復号
登録内容の確認

図11

フロントページの続き

(51) Int. Cl.[6]		識別記号	FI		
Ｈ０４Ｎ	1/00	１０７	Ｈ０４Ｎ	1/32	Ｚ
	1/32			1/44	
	1/44		Ｈ０４Ｌ	9/00	６７５Ｂ